SPECIFICATION

Please replace paragraphs [0011], [0012], [0032] and [0033] (as published in Pub. No. 2004/0218763) with the following amended paragraphs:

[0011] The first private key may be disabled when the second private key is used for authentication. In addition, a third private key associated with the second private key and a third public key corresponding to the third private key may be created. The third ~~public~~ private key may be output once such that it can be re-created. The third private key may then be re-created and used for authentication. Alternatively, the use of the second private key for authentication may be disabled and the third private key may be used for authentication. The ~~second~~ third private key may then be re-created and used for authentication.

[0012] The method may further comprise creating a third private key associated with the second key and creating a third public key corresponding to the third private key; creating a fourth private key associated with the third private key and creating a fourth public key corresponding to the fourth private key; outputting the fourth private key once such that it can be re-created; and outputting the third and fourth public keys. The use of the second private key for authentication may be disabled and the third private key used for authentication. The fourth private key may then be re-created and used for authentication. Furthermore, outputting the second ~~public~~ private key may comprise creating at least two shares of the second ~~public~~ private key and outputting each share once to a different entity.

[0032] Figure 2 shows a method 200 for generating keys for public key cryptographic systems. Processor ~~114~~ 112 creates (210) a first set of keys, i.e. a first private key and corresponding first public key. Processor ~~114~~ 112 also creates (220) a second set of keys, i.e. a second private key and corresponding second public key. The second set of keys is associated with the first set of keys. However, the second set is created independently from the first set. The keys may be generated using various algorithms known in the art.

[0033] For example, the keys may be generated based on the well known Digital Signature Standard (DSS). Here, processor ~~114~~ 112 uses an internal source of randomness to create a private or secret key x to be used for DSS. A corresponding public key X is then calculated as follows, where P is a large prime number, for example 1024 bit, that defines a mathematical field in which the mathematical operations take place, Q is another prime number, typically of 160 bits or more, such that $Q|(P-1)$, and g is an element of the field and is a generator of the order-Q subgroup of F*(P).